الجمهورية الجزائرية الديمقراطية الشعبية

People's Democratic Republic of Algeria

Ministry of Higher Education and Scientific Research

National School of Cyber Security

Foundation Training Department

وزارة التعليم العالي والبحث العلمي

المدرسة الوطنية العليا في الأمن السيبراني

قسم التكوين القاعدي

LEVEL : 1st Year Basic Training

SECTION / GROUP : A & B

MODULE : Algebra 1

FULL NAME : ....

MODULE'S TEACHER : Dr. Hamza Moufek

DATE : 13 / 01/ 2025

DURATION : 2h

NOTE : No documents are allowed.

Midterm Exam

Exercise 1 : (3,5 points)

In this exercise, we aim to show the existence of a non-integer real number x, such that :

$$\forall n \in \mathbb{N}, \quad x^n + \frac{1}{x^n} \in \mathbb{Z}.$$

1. Let $x \in \mathbb{R}^*$. Assume that $x + \frac{1}{x} \in \mathbb{Z}$. Using the following equality

$$\forall n \in \mathbb{N}, \left(x^{n+1} + \frac{1}{x^{n+1}}\right)\left(x + \frac{1}{x}\right) = \left(x^n + \frac{1}{x^n}\right) + \left(x^{n+2} + \frac{1}{x^{n+2}}\right),$$

show that for all $n \in \mathbb{N}$, we have :

$$x^n + \frac{1}{x^n} \in \mathbb{Z}.$$

2. (a) Show that there exists an integer $x \neq 0$ such that $x + \frac{1}{x} \in \mathbb{Z}$.

   (b) Show that there exists a non-integer real number x, such that $x + \dfrac{1}{x} \in \mathbb{Z}$.

3. Conclude. $\exists x \in \mathbb{R} - \mathbb{Z} : x + \frac{1}{x} \in \mathbb{Z}$

4. Does there exist a complex number x with non-zero imaginary part, such that $x + \dfrac{1}{x} \in \mathbb{Z}$?

$\forall x \in \mathbb{R} \setminus \{\mathbb{Z}\} : x+$

Exercise 2 : (2,5 points)

Let the function

$$f_a : \mathbb{R}^2 \to \mathbb{R}^2, \quad (x, y) \mapsto (ax - a^2 y, y),$$

where a is a nonzero real parameter.

1. Show that the function f_a is bijective. Determine its inverse.
2. Find a condition on a and b such that :

$$f_a \circ f_b = f_b \circ f_a.$$

3. Determine (without proof) the expression for $f_a^{(n)}$ for $n \in \mathbb{N}^*$. (Recall that $f_a^{(n)} = \underbrace{f_a \circ f_a \circ \cdots \circ f_a}_{n \text{ times}}$, for $n \geq 1$).

Exercise 3 : (5 points)

Let $n \geq 2$ be a natural number. We define :

$$U_n = \{z \in \mathbb{C}^* \mid z^n = 1\}.$$

1. Show that U_n is a subgroup of $(\mathbb{C}^*, \cdot)$.
2. Let φ_n be the function defined by :

$$\varphi_n : U_n \to U_n, \quad z \mapsto \varphi_n(z) = z^2, \quad \forall z \in U_n.$$

   Show that φ_n is a group endomorphism.
3. (a) Determine $\ker(\varphi_4)$. Is φ_4 injective?
   (b) Determine $\ker(\varphi_5)$. Is φ_5 injective?
   Justify your answers.

Exercise 4 : (9 points)

We denote $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$, where i is the complex number such that $i^2 = -1$.

1. Show that $(\mathbb{Z}[i], +, \cdot)$ is a subring of $(\mathbb{C}, +, \cdot)$.
2. Let $N : \mathbb{Z}[i] \to \mathbb{N}$, $z \mapsto z\overline{z}$; where $\overline{z} = a - ib$.

   a+b ∈

   (a) Justify that $N(\mathbb{Z}[i]) \subseteq \mathbb{N}$.
   (b) Show that $N(z \cdot z') = N(z) \cdot N(z')$, $\forall z, z' \in \mathbb{Z}[i]$.
3. Let $\mathbb{Z}[i]^*$, the set of units in $\mathbb{Z}[i]$ whose inverse is also in $\mathbb{Z}[i]$. Alternatively written :

$$\mathbb{Z}[i]^* = \{z \in \mathbb{Z}[i] \mid \exists z' \in \mathbb{Z}[i], zz' = 1\}.$$

   (a) Show that $\mathbb{Z}[i]^* = \{z \in \mathbb{Z}[i] \mid N(z) = 1\}$.
   (b) Deduce all elements of $\mathbb{Z}[i]^*$.
4. We denote $\mathbb{Q}[i] = \{a + ib \mid a, b \in \mathbb{Q}\}$. The ring $(\mathbb{Q}[i], +, \cdot)$ is it a field?
5. We say that z divides z' in $\mathbb{Z}[i]$ if there exists $q \in \mathbb{Z}[i]$ such that $z' = qz$. We denote this as $z \mid\mid z'$ (thus defining a reflexive and transitive relation on $\mathbb{Z}[i]$).
   Remark : we always denote $m \mid n$ for the divisibility relation in $\mathbb{Z}$.
   (a) Let z, z' be two elements of $\mathbb{Z}$, hence of $\mathbb{Z}[i]$. Show that $z \mid z' \iff z \mid\mid z'$.
   In other words, the divisibility relation in $\mathbb{Z}[i]$ "extends" that of $\mathbb{Z}$.
   (b) Let z and z' be in $\mathbb{Z}[i]$. Show that $(z \mid\mid z'$ and $z' \mid\mid z) \iff \exists u \in \mathbb{Z}[i]^*, z' = uz$.
   We express this situation by saying that z and z' are *associated* in $\mathbb{Z}[i]$.
   Throughout the following, we denote $z \sim z'$ to indicate that z and z' are associated.
   (c) Show that the relation $\sim$ is an equivalence relation on $\mathbb{Z}[i]$.
   We denote $cl(z)$ as the equivalence class of an element z of $\mathbb{Z}[i]$.
   What is the cardinality of $cl(z)$? What does $cl(z)$ represent geometrically?

z.z̄